NAVAL WAR COLLEGE
Newport, R.I.

WAR ON THE CHEAP: USING INFORMATION WARFARE TO LENGTHEN THE DECISION CYCLE

by

Thomas H. Carr, Jr.

Major, U.S. Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature:

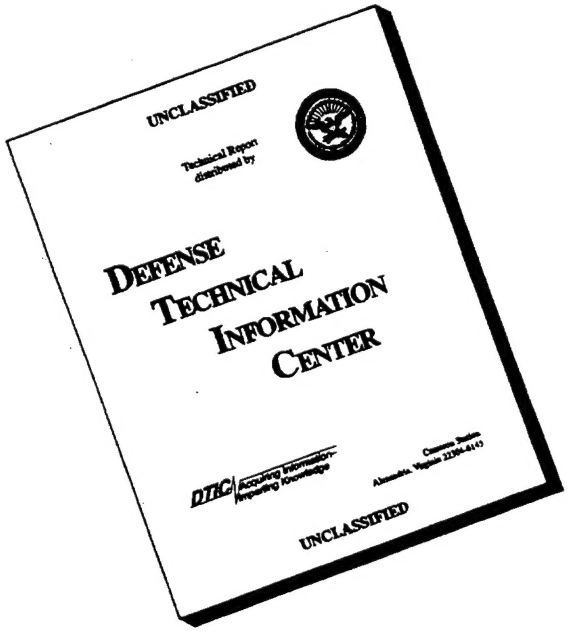
14 June 1996

Paper directed by Captain D. Watson
Chairman, Joint Military Operations Department

Faculty Advisor
Captain George W. Jackson

Date

DISCLAIMER NOTICE



THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization: JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: 1C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification):
War On The Cheap: Using Information Warfare To Lengthen The Decision Cycle (U)

9. Personal Authors: Carr, Thomas H. Major, USA

10. Type of Report: FINAL

11. Date of Report: 12 February 1996

12. Page Count: 25

13. Supplementary Notation: A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

14. Ten key words that relate to your paper: Information Warfare, Computers, Operations, Tempo, Technology, Hacker, Force Projection, Decision Cycle, O-O-D-A Loop, Digital

15. Abstract: This paper investigates how an adversary of the United States might indirectly attack a center of gravity of a United States military operation by disrupting operational tempo using information warfare. Current military doctrine mandates quick and decisive victories whenever United States Forces are called to combat. A key element of this doctrine is the creation of an operational tempo that an enemy cannot match and so defeating him quickly with as few casualties as possible. The doctrine reflects a political reality that the American public will not support protracted and indecisive conflicts with large numbers of casualties. It is also a fact that most future United States military operations will project forward from the continental United States to immature theaters of operations. The combination of the requirements for high operational tempo and power projection from the United States will demand much from our information technology. Automated support systems for administration and logistics will be key to any future successful operation. This paper will not discuss how information resources are used by the United States but how a potential adversary might be able to manipulate these resources to disrupt operational tempo. This paper will show how a financially limited country could effectively fight the United States military, not by buying expensive exotic weapons systems, but by paying talented computer hackers and others familiar with United States support networks to disturb these systems. A good information warfare capability such as this would be a great combat multiplier for any foe and is not a capability realized sufficiently by United States military joint planners.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-[redacted] 6461 | 20. Office Symbol: C

Abstract of

War On The Cheap: Using Information Warfare To Lengthen The Decision Cycle

This paper investigates how an adversary of the United States might indirectly attack a center of gravity of a United States military undertaking by disrupting operational tempo using information warfare. Current military doctrine mandates quick and decisive victories whenever United States Forces are called to combat. A key element of this doctrine is the creation of an operational tempo that an enemy cannot match and so defeating him quickly with as few casualties as possible.[1] The doctrine reflects a political reality that the American public will not support protracted and indecisive conflicts with large numbers of casualties. It is also a fact that most future United States military operations will project forward from the continental United States to immature theaters of operations. The combination of the requirements for high operational tempo and power projection from the United States will demand much from our information technology. Automated support systems for administration and logistics will be key to any future successful operation. This paper will not discuss how information resources are used by the United States but rather how a potential adversary might be able to manipulate these resources to disrupt operational tempo. This paper will show how a financially limited country could effectively fight the United States military, not by buying expensive exotic weapons systems, but by paying talented computer hackers and others familiar with United States support networks to disturb these systems. A good information warfare capability such as this would be a great combat multiplier for any foe and is not a capability realized sufficiently by United States military joint planners.

INTRODUCTION

The more the data banks record about each one of us, the less we exist.
Marshall McLuhan (1911–1980), Canadian communications theorist. *Playboy* (Chicago, March 1969).

Emerging enemies of the United States can efficiently enhance their strength with modest investments in information warfare capability rather than buying expensive military hardware. The power of information warfare can lengthen an American joint force commander's decision cycle interrupting the tempo he wishes to impose upon that enemy. Information technology has added a dimension to warfare that the operational commander is not prepared for and vulnerable to.

The military of the United States is the most powerful in the world today. Since the demise of the Soviet Union in the early 1990's, no single country can match her military might dollar for dollar or pound for pound. The fact is that today conflict tends to come in the regional rather than global form. The adversaries the United States will face soon will look more like Iraq, Iran or North Korea rather than the former Warsaw Pact countries of the Cold War. Operation DESERT STORM proved to the world that no third world country could engage in conventional warfare with the United States military and prevail. Our forces were too numerous and too technologically advanced for even a country such as Iraq who possessed a larger army than the United States fielded against them. How might such a country contend with a force such as America's? An answer might lie in the realm of Information Warfare.

This paper will explore what I believe to be a critical vulnerability for a joint force commander fighting a Major Regional Contingency (MRC) as envisioned by the 1993 Bottoms Up Review. By hiring computer hackers and other experts familiar with automated

systems which provide logistics and personnel support to United States military forces, an adversary could disrupt the operational tempo of the joint commander. This approach would indirectly attack a United States center of gravity by denying the quick victory needed to maintain popular support for any combat expedition. Public opinion is a strategic center of gravity for the United States. Quick decisive victories maintain favorable public support.[2] These rapid victories are attained through the maintenance of an operational tempo that an enemy cannot match.[3] This tempo is an operational center of gravity, and superior information technology makes it possible and sustains it. The manipulation or disruption of military information systems can slow tempo, delay the victory, and erode public support. While it is true that tempo is also maintained by other factors such as mobility, command and control and intelligence, the logistics and personnel support information systems of our military provide a softer target for enemy exploitation.

MANY PATHS, LIMITED MEANS

Along the spectrum of warfare there are many ways an adversary might attack the United States; however, he must choose a way that is within his means. A large conventional force is one of the more traditional ways. The conventional military forces of today, however, are very expensive and difficult to maintain. Only a global superpower can do it and even then it is difficult. The Soviet Union was in large part destroyed because of the disproportional diversion of their national resources to the military. The United States incurred a massive debt that she struggles with today to pay for the large military she built and then partially dismantled in the 1980's and '90's.[4] The purchase of hardware for a country's defense is but a small part of the total outlay needed to develop an adequate conventional capability. Iraq

bought multitudes of military hardware, but then neglected to thoroughly train their soldiers, leaving them ineffective in operating the weapons that had been purchased for them.

Another method used by smaller countries to oppose militarily superior adversaries is terrorism. This is a very cost effective means of conflict and figured largely in the 1973 Yom Kippur War fought between Israel, Egypt and Syria. The Munich Olympic Massacre of 1972, carried out by the Palestine Liberation Organization (PLO), arrested the Israeli intelligence acuity and allowed the Egyptian Army to completely surprise the Israeli Army with their dash across the Suez Canal.[5] Terrorism can backfire, however, and cause military reprisals against the states who sponsor it. This was a hard truth learned by Libya in 1986 when the United States bombed several military and political targets in retaliation for the LaBelle Discotheque bombing in Berlin that killed and wounded several Americans. Terrorism is probably not very effective at the operational level of war and is better suited for the strategic level.

An alliance with another superpower can be yet another way for a small country to oppose a larger one. The cost in this case could be rather large as well, with economic dependence or relinquishment of some sovereignty being the bill to pay. Cuba suffered both these consequences by acquiescing to the posting of Soviet troops on her soil and depending on the Soviet Bloc as the only purchaser of her sugar crop. When the Soviet Union fell in 1991, it not only left Cuba in an economic lurch from which she has not recovered, but also left her unprotected militarily as the former alliance today could not help her should she find herself in a war with the United States.[6]

Finally, a country with neither powerful allies nor well trained and equipped armies could use information warfare to attack the operational centers of gravity of the United States. This option would be cheaper to use both politically and financially.

DOCTRINE, TEMPO, AND THE DECISION CYCLE: THE VULNERABILITY

Doctrine is simply the way that someone wishes to fight a war. The way the United States Army wishes to fight a war can be found in Field Manual (FM) 100-5 entitled Operations. Two principles contained in this doctrine that are crucial to this paper's thesis are force projection and tempo.

Force projection is "The movement of military forces from CONUS to a theater in response to requirements of war or operations other than war."[7] Force projection represents a shift from the Cold War forward deployment of forces overseas. This means that future United States operations will start with a deployment from the Continental United States (CONUS) to a foreign theater of operations. This theater may be mature or immature, with more logistical support required for the immature variety. Limited sea and airlift resources will demand that a small logistics "tail" be brought to the theater and that the bulk of transportation assets be used to bring the operational "teeth" to the area first. Once the force has deployed to the theater of operations the transportation assets must then provide the sustaining logistics in the most efficient manner possible. The United States Army has developed two important new logistics doctrines: split-based operations and total asset visibility. Split-based operations will allow the bulk of sustainment forces to remain in the United States supporting the deployed force through electronic data exchange. Total asset visibility will track the movement of supplies to the forward area through automated methods

such as bar coding that feeds back into the logistical computer systems.[8] New logistical demands are as never before: a World War I Infantry Division required 100 tons of supplies per day, a World War II Armored Division 300, and the Mechanized Infantry Division of today over 1,500 tons a day.[9] Split-based operations will move these required supplies directly from CONUS to the theater of operations with strategic air and sea lift. Since the United States possesses limited air and sea lift capacity, each plane and ship must be loaded with only the most needed supplies to maximize efficiency. Coordinating this sustainment effort from widely dispersed depot and supply activity locations in CONUS can only be done efficiently with information systems linked together with shared databases for synchronism. This logistics doctrine has been called a "Wal-Mart war"[10] in which computers linked by communications do for military logistics what they have done to keep supermarkets supplied for fast sales. These logistics networks such as the United States Army's Objective Supply Capability (OSC) will be vital to sustain any force past the limited basic supply loads they bring with them to the theater. The reliance on automation and communications makes these systems critical vulnerabilities that an adversary might attack and disrupt. The more our military forces come to depend on information systems, the more difficult will it be for them to do without them. Any return to a fallback mode, whether partially automated or manual will result in decreased capability.[11] Lieutenant General Paul Menoher, Army deputy chief of staff for intelligence states, "If our combat processes are totally tied to the ability to pass information through certain systems to certain points within a certain time frame, anyone who can interrupt that flow diminishes our advantage."[12]

Tempo is the rate of military action; controlling or altering that rate is a necessary means to initiative; all military operations alternate between action and pauses as opposing forces battle one another and fight friction to mount and execute operations at the time and place of their choosing.[13] The commander creates a tempo that his adversary cannot match by acting more rapidly than his opponent can. A person's ability to act is an iterative process defined by one author as an observation-orientation-decision-acting or O-O-D-A loop.[14] The shorter the loop the faster you act, and if your decision loop is smaller than your opponent's then he is forced to react to your actions and loses initiative. Figure one illustrates this state. Once this state has been achieved by a combatant it has the effect of accelerating time for his opponent, eventually to the point where he can no longer make effective decisions but must simply react to whatever situation is created for him.

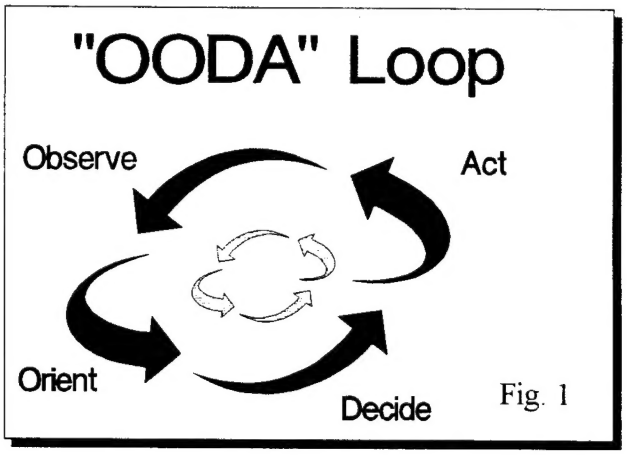


Fig. 1

Information technology is the enabler of smaller diameter decision cycles. Automated, smart logistic and personnel support systems will decrease the length of operational pauses. Using the Wal-Mart War analogy which is also known in the private sector as "Just in Time" we can resupply combat units with personnel, ammunition, fuel, food and repair parts at the very moment they are needed with less diversion of resources to the resupply effort. Technology will allow our forces to surge their combat power more often and over greater distance than ever before. The operational tempo will at that point be limited only by the physical endurance of the individual soldier.

This great technical capability, however, brings with it great fragility as an unintended consequence.[15] This fragility and the capability to exploit that weakness has been demonstrated many times in the past, but a recent event reported by *Defense News* illustrates the vulnerability. The article reported that a United States Air Force captain, using a personal computer and modem, penetrated the command and control system of United States Navy ships operating in the Atlantic Ocean. This intrusion was done with the permission and knowledge of the Navy to determine vulnerabilities in their ship board systems. Once inside the network, the captain found his way into the ship's command and control systems and could have given the ship incorrect navigational headings. The Air Force operators used the commercial Internet to gain access to the Navy's network with equipment that any person could have purchased in the private sector.[16] Logistics support networks like the Army's OSC system are also connected to commercial systems that could be used as a pathway to penetration.

In December 1995, a hacker was able to gain access to a computer system at the Naval Post Graduate School (NPS) in Monterey California. He gained access to the control element of the NPS's UNIX server, which runs all the school's computer networks including one known as the Command, Control, Communications, Computer and Intelligence professional (C4I-Pro) network bulletin board. Programs were placed in the computer host which would gain user passwords and transmit them back to the hacker.[17] This particular penetration illuminates an inherent weakness of the UNIX computer operating system. First designed by AT&T Bell labs in the 1970s, it was used extensively by colleges and universities and was considered an "open" system which did not lend itself well to security which would

keep the system "closed" or resistant to intrusion. UNIX is the system of choice for many DoD information systems today.

The following paragraphs illustrate our vulnerability by describing a possible scenario in which a financially limited country uses information warfare to attack United States' centers of gravity. Country X seizes a strategically important strait or other passage and prohibits other countries, including the United States, from passing through the area. The United States responds with the deployment of a Joint Task Force (JTF) to the area to reopen the passage. The country has smaller and less capable armed forces than the United States but has anticipated our response. Prior to the seizure of the area, Country X's intelligence service had scouted various colleges and universities and looked about on electronic bulletin boards on the Internet obtaining the services of some rather competent computer hackers. The sums of money offered these hackers was modest in proportion to Country X's national budget, but very large to the unemployed student hackers. Country X's political leadership had decided in advance to take advantage of availability of hackers for hire and to use them to augment their combat efforts. Country X decided to "buy and use" hackers as weapons rather than purchase additional expensive and complex military hardware. Their armed forces remained modest but their combat effectiveness is increased at low cost by the use of these individuals.

Country X began their campaign well before the start of open hostilities. First, their intelligence service obtained unclassified user, operator, and doctrinal manuals for the targeted logistics and personnel systems. From these manuals and publications a rather precise understanding of the functionality of the targeted systems was obtained. The hackers could tell how the systems "talked" to one another and what function (fuel, ammunition, food) they

served for United States military forces. Next the hackers Country X had hired began to penetrate the network that the support systems used and left "trapdoors" or ways to reenter the systems at a later time on each database they could penetrate. Once the hostilities began the hackers monitored each of the databases they had entered and watched the pattern of logistics requests and release orders that were processed. From these patterns it is easy to tell what was being requested for the theater of operations. Meanwhile, the armed forces of Country X attacked the Joint Task Force but remained indecisively engaged prolonging the conflict. Now the information warriors of Country X begin to alter personnel and supply requests and issues that the systems they had penetrated produced. The Joint Task Force exhausts its basic loads of supplies it initially brought along. Resupply from CONUS is now required to keep the operational tempo going at a rate Country X can not match. However, instead of receiving ammunition, food and fuel, supply ships and air lift show up with the wrong supplies. The Joint Task Force finds it very difficult, if not impossible, to sustain the tempo of the operation and must now verify each supply transaction manually. The result is that the fighting is prolonged, robbing the JTF Commander of the quick decisive victory he desires. The protraction of the fighting causes causalities to mount and erodes public support to continue the operation. The United States, which began the conflict with great self-assurance of a rapid victory, is forced to reconsider its policy in the area.

The JTF used manual backup features for their computing systems, but as former Vice Chief of Staff of Naval Operations Adm. (ret) Stan Turner has said, "Using those manual backup systems robs the commanding officer of the operating speed inherent in the automated

systems. It is the speed of operations that gives the United States ... an advantage over potential enemies."[18]

HACKERS: CHEAP WEAPONS

Since I have proposed computer hackers as effective cheap weapons, we should examine the weapons themselves. How reliable would hackers be to a country who hires them? Are hackers competent and how would you control them once they were engaged? Where would you find them? At what sorts of missions would they be most effective at doing? Will hacker warfare be decisive?

Although no definitive study of the psychology of hackers was found during my research, a sort of personality profile emerges from recent cases. Included in Appendix A is a non-academic description of hacker personality traits which was downloaded from a popular hacker electronic bulletin board. This description was written by a hacker and provides some insight into hacker psychology. Hackers are very intelligence and intuitive but the sense of challenge and curiosity are probably their defining attributes. Hackers tend to live for "the game" of intruding on protected systems, lurking about and then leaving without anyone knowing they were there. One of the most famous intrusions by the "Morris Worm," a computer virus which brought the Internet to its cybernetic knees was really intended as a harmless prank.[19] Competitiveness, resistance to authority and the belief that all information should be free and open are the right attributes that a foreign intelligence agency would be looking for in a recruit. Add to that mix the prospect of significant financial reward and the recruitment of such individuals would seem rather simple to accomplish. This would appear to the hacker recruit as "getting paid for having fun." However, the personality traits of

hackers, such as the dislike of authority could work against their masters requiring non-authoritative management, slowing responsiveness. Reliability of the hirelings due to a lack of discipline would be a problem, so their progress and success would have to be monitored by the interested government. However, traditional weapons systems purchased through the world arms markets are also prone to failure, particularly when the training for the use of these weapons is cursory. This was experienced by the Argentines during the Falklands war. Their West German torpedoes were fired within the proper range and speed parameters, but were not mated properly to their submarine's fire control and missed lucrative British targets.[20] Here the hacker would prove easier to control than the large numbers of technicians needed to train the armed forces of the weapons buying country. The hacker would come fully trained as it were and require little "spin up" time to be ready for use. The hacker would continue to do what he had been doing prior to his recruitment, hacking into protected systems. Control would probably be exercised through psychological manipulation by the hiring country's intelligence service with a combination of fear and financial reward.

The place to find most hackers would be through electronic bulletin boards on the Internet where the hacker elite tend to congregate (e.g.. http:\\www.10pht.com: LOpht Heavy Industries).[21] Initial contact could be through the Internet with personal follow up by intelligence agents for final choice and recruitment.

There would be two basic missions for the newly recruited hacker. The first would be a careful study of the architecture and function of the system he was assigned to penetrate. Attempts to attack any system without previous knowledge of its basic architecture and function would be little more than a shot in the dark.[22] Understanding the architecture entails

knowing who the system is connected to and how it communicates. The function of the system is what it does and how the database is structured. This information is typically completely unclassified and can be found in any government technical library such as the Defense Information Technical Center (DTIC) and its publications. For instance, the United States Army requires a full and complete description of the database structure and data elements of all its Standard Army Management Information Systems (STAMIS) in the systems documentation. This documentation, which is very detailed and complete, is totally unclassified and available on open government electronic bulletin boards or through the contractors who wrote them.[23] The hacker would, for instance, need to know and understand the National Stock Number (NSN) system and the noun nomenclatures in order to manipulate a database and change a requisition from 100 gallons of aviation fuel to 100 gallons of heating oil.[24] Armed with this knowledge, the hacker could manipulate the database to issue or not issue supplies, or do whatever necessary to produce the desired effect on the operation once he had penetrated the system.

The second mission for the hacker would then be the penetration of the targeted systems and the attainment of system administrator powers. Listed below in a table are a sample of some mechanisms that hackers use to penetrate and gain control of automated systems. Once inside the system the hacker would take care not to do anything that would alert the system administrators to his presence and would simply wait until it was time to act.

Technique	Procedure	Result
Trojan Horse	False login screen presented to user.	Login ID and Password are e-mailed to hacker for use later. User thinks he just had a faulty login attempt and continues on.
Sniffer	Program inserted in the operating system that finds and copies password files.	Hacker then uses deencryption program (many are public domain) to obtain system administrator's password. In the UNIX operating system this password is called "root."
Backdoor	A hole in the security of a system deliberately left in place by designers or maintainer.	Contains code that would recognize when the `login' command was being recompiled and insert some code recognizing a password chosen by the hacker, giving him entry to the system whether or not an account had been created for him.

The strategy of using hackers as part of the combat operation by a foreign government would require advance planning and time to implement, which would negate hasty attacks. Information warfare of the hacker variety would be effective at the operational level of war only after careful pre-hostility planning and design.

The decisiveness of this type of warfare would be very low if left to itself. I must stress that this type of warfare, like so many others, must be used in concert with other means. An adversary of the United States would still need a somewhat capable conventional armed force that could deliver steel as well as electrons against naval, air and ground forces. However, the crucial benefit information warfare offers is its great cost to effect ratio. For example, compare the effect of a single SILKWORM missile and the associated cost of training and related infrastructure to fire it versus the cost to pay a small group of hackers and equip them with commercially purchased computer equipment. Compare the maximum damage that one missile could inflict on the naval battle group — one ship sunk versus the paralysis inflicted on the entire JTF by hacker interference with false navigation inputs or

inadequate sustaining supplies delivered to them. The promise of information warfare is more "bang for the buck." Hacker warfare would not replace weapons systems but complement them in attacking the opponent's center of gravity. The effects of information warfare would be felt at the operational level of war, but could impact the strategic level as well. As posed in the Country X example, prolonging any conflict with the United States tends to work for an adversary by eroding American public support for the operation.

Clearly the best targets for these new information warriors would be those with the least security and with connections to unclassified commercial communications.[25] These are often logistics systems that require access to civilian systems for procurement proposes. Most of these systems can be reached directly through the Internet using the TELNET communications protocol. Manipulation of supply requisitions, and input of bogus navigational signals into a ship's command and control systems would be most effective and afford the attacker the least chance of being discovered.

Destruction of the system through virus or erasure of information on the host computers can work as well. Computer viruses could be delivered via electronic mail as America On-line users recently discovered.[26] Equally as devastating would be the hacker who obtained system administrator capabilities and then destroyed file systems and data files by simply deleting them.

HACKER WARS: THE FINAL BATTLEFIELD?

The purpose of this paper is not to present a Hollywoodesque drama of international hackers waging successful war against contemporary military forces. Indeed, with movies such as The Net and Hackers along with several popular books and magazines, the tendency is

to exaggerate the actual effect of information warfare. Information warfare will be valuable when used in conjunction with traditional military operations and should be a planning factor for the operational commander. I do not believe that information warfare will be sufficient by itself in military operations, rather it will serve as a combat multiplier, an effect that is far greater than either its cost or the energy required to perform it.

There are some things to consider when planning to use or defend one's self against information warfare. First, isolated information is no good to those who cannot reach it. It serves little purpose to wall off vital data from the forces who need it. Protection does not mean sequestration. Prudent measures would include information systems being routinely tested by their owners to determine existing vulnerabilities. The worst possibility is the system administrator who becomes overconfident and thus makes his system ripe for intrusion. The use of such tools as the public domain SATAN software program, which detects vulnerabilities in UNIX based computer systems, was very helpful to the 5th Signal Command where I was stationed as an operations officer from 1993-5. Internal security systems (e.g. COPS) that run on the host computers operating system, detect repeated unsuccessful login attempts from unknown hosts, and report them to the systems administrator are advised. Second, the support databases in the United States can be checked to identify manipulated data entries. Certain parameters built into databases called edit tables can detect obviously wrong requisitions that a hacker would try to substitute while manipulating the system. These edit tables would flag the supporting supply agencies when abnormal requests were made such as someone ordering several hundred iterations of a repair part. These edit tables exist today in many databases and could be tailored to specific units (e.g. no aircraft fuel for a tank unit)

or to a specific type of operation. Redundancy in systems through distributed databases will allow computers to hand off and take over for one another if hackers crash a particular system. Robustness of networks and systems with communications and database redundancy makes critical links less so and provide multiple paths for the restoral of disrupted service. Further designs that physically distribute shared databases down to the operational level from the strategic level will help to protect information without isolating it from the information resources in CONUS. Operational locally owned and operated databases would mirror the information in CONUS databases that pertained to its operation. The local staff could "see" what was going on in CONUS systems that were germane to their units. This lower level of control would allow the operational commander's staff to monitor logistics transactions and discover any that were manipulated. An added bonus would be catching mistakes that their own operators had inputted by the reports the commander's staff generated locally.

Hacker intrusion into vital information systems should be on the operations order planning checklist for any military enterprise in the Information Age. Operational commanders must also keep alive those manual skills that are vital to their warfighting ability. Foolish indeed would be the naval officer who did not insist that his sailors be able to navigate celestially but who relied solely on the Global Positioning System. Likewise, logistical planners must foresee computer breakdowns, whether hacker initiated or not, and have viable workarounds. We should remember that the one computer no hacker can penetrate is the one we humans are born with— our own brains.

APPENDIX A

"A Portrait of J. Random Hacker" downloaded from an electronic bulletin board (This page hosted on the ISC WWW server) on the Internet that many "hackers" like to frequent. This is a description of hacker personality by a self professed hacker.

This profile reflects detailed comments on an earlier `trial balloon' version from about a hundred USENET respondents. Where comparatives are used, the implicit `other' is a randomly selected segment of the non-hacker population of the same size as hackerdom.

Personality Characteristics

The most obvious common `personality' characteristics of hackers are high intelligence, consuming curiosity, and facility with intellectual abstractions. Also, most hackers are `neophiles', stimulated by and appreciative of novelty (especially intellectual novelty). Most are also relatively individualistic and anti-conformist.

Although high general intelligence is common among hackers, it is not the sine qua non one might expect. Another trait is probably even more important: the ability to mentally absorb, retain, and reference large amounts of `meaningless' detail, trusting to later experience to give it context and meaning. A person of merely average analytical intelligence who has this trait can become an effective hacker, but a creative genius who lacks it will swiftly find himself outdistanced by people who routinely upload the contents of thick reference manuals into their brains.

Contrary to stereotype, hackers are not usually intellectually narrow; they tend to be interested in any subject that can provide mental stimulation, and can often discourse knowledgeably and even interestingly on any number of obscure subjects --- if you can get them to talk at all, as opposed to, say, going back to their hacking. It is noticeable (and contrary to many outsiders' expectations) that the better a hacker is at hacking, the more likely he or she is to have outside interests at which he or she is more than merely competent. . They tend to be attracted by challenges and excited by interesting toys, and to judge the interest of work or other activities in terms of the challenges offered and the toys they get to play with.

Hackers have relatively little ability to identify emotionally with other people. This may be because hackers generally aren't much like `other people'. Unsurprisingly, hackers also tend towards self-absorption, intellectual arrogance, and impatience with people and tasks perceived to be wasting their time. As cynical as hackers sometimes wax about the amount of idiocy in the world, they tend by reflex to assume that everyone is as rational, `cool', and imaginative as they consider themselves. This bias often contributes to weakness in communication skills. Hackers tend to be especially poor at confrontation and negotiation.

Hackers are often monumentally disorganized and sloppy about dealing with the physical world. Bills don't get paid on time, clutter piles up to incredible heights in homes and offices, and minor maintenance tasks get deferred indefinitely. The sort of person who uses phrases like `incompletely socialized' usually thinks hackers are. Hackers regard such people with contempt when they notice them at all.

APPENDIX B

The following article was downloaded from the Internet at: http:\\www.10pht.com.

THE REAL FILE FOR ATM THEFT !! WRITTEN BY: THE RAVEN

III. ELECTRONIC & COMPUTER SCAMS

Scarcely a week goes by that I don't hear about one scheme or another successfully used by phreaks & hackers to penetrate large systems to access data banks and to perform various manipulations. Although we have only been able to verify one or two of the methods that we will describe, numerous cases have arisen in recent years in which an ATM was defrauded with no evidence of a hardware or software bug to account for the robbery.

The outlaw can use several approaches. One is to use wiretapping. Another is to obtain the secrets of the cipher, or hardware or software defeats to the system and proceed accordingly. Another one that works with banks is to set up phony debit accounts and program the computer to believe that the debit accounts are full of money. Then when a three day weekend comes around proceed with friend to deplete all of these debit accounts by making various rounds to ATMs. Electronic frauds of ATMs require an excellent technical understanding of phone and-or computers all of which you can obtain from worthy underground news letters such as TAP, and 2600, etc. OR from a H/P BBS. "Tapping" or "wiretapping" consists of the unauthorized electronic monitoring of a signal (voice or digital) transmitted over a phone or computer (commo) circuit.

A "tap" is the monitoring device that does this. Although a tap is usually placed somewhere on a phone line or junction box, it may be placed inside of a phone, modem or computer. With the advent of isolated stand-alone ATMs (with vulnerable phone lines, including POS terminals) and computer technology. The phone circuits that connect ATMs to their host computer (located in the banks data processing center) can be tapped anywhere between the two.

An "invasive tap" is one in which a hard electronic connection is made between the tap and the commo circuit. A "non-invasive" tap is one in which an induction loop or antenna is used to pick up the EMI generated by the signal, and there is no physical connection between the commo circuit and the line. A "passive tap" is one in which the tap simply transmits to a recorder or directly records the tapped signal and in no way interferes with it. An "active tap" is one in which the tap ALSO interferes (changes, adds to or deletes) the tapped signal in some way. Active taps are more sophisticated. Atypical ATM active tap is one that records a signal, the later plays it back over the line. Be sure to look for my text "HIGH TECH TOYS." It lists where to get things that are VERY hard to get or things that you may need a license to obtain without those hassles. All you need will be money!

Method 1. PASSIVE TAPS All tapped ATM transactions are recorded over a period of time (but not interfered with). Once the serial protocol and MA codes are understood, the transmitted data is decrypted (if encrypted) using known entry data to the ATM. Note that some systems use a MA code that is complex and very difficult to crack. Messages to and from the ATMs host computers are composed of various fields. One field identifies the transaction type, one the PIN, one the PAN, one the amount, one the approval code, one the transaction number and perhaps other fields. In most systems, either nothing is encrypted or

only the PIN field. In others, the entire message is encrypted. The ATM/host circuit is monitored over a period of time to detect PINs, PANs and other entry data of other ATM users based upon (decrypted) transmitted data. Phony debit cards are then made to defraud ATM accounts with known PINs and PANs.

Method 2. ACTIVE TAPS Active tapping is one method of spoofing. The critical part of the host computer's message are the approval and amounts fields. The critical parts of the ATMs transmission are the continuous transmission it makes to the host computer when NO one is using it to indicate that it is OK, and the PIN and amount fields. Both good and bad cards and good and bad PINs are entered at various times and days to differentiate between the various massage components. Various quiescent periods is also recorded. Once the message structures are understood, a computer is then substituted to act as both the host computer and the ATM. That is, a computer is then connected between the ATM and the host computer. This computer acts like the host computer to the ATM, and like the ATM to the host computer. An accomplice uses the ATM to go through the motions of making legitimate transactions. If his procedures are correct, the ATM communicates, with the host computer for permission to discharge the money.

Several methods: (A) The phreaker changes the approval field in the hosts message to OK the transaction regardless of its real decision. The phreaker may interdict the message regardless of its real decision. The phreaker may interdict the message from the ATM to tell the host that the ATM is inactive while interdict the host message to tell the ATM to disburse the cash. Since the ATM is no longer connected to the host computer, and the host computer believes that it is talking to an unused ATM (or one engaged in balance inquiry transaction), no moneys will be deducted from any debit account, no denials will be made based upon daily maximum limits, and no alarm will be sounded due to suspicious behavior. Even if the ATM sounds an alarm, the host computer won't hear it as long as the phreaker is whispering sweet nothings into its ear. Also by using this method, as long as the PIN & PAN check digits are legitimate ones based upon the ATMs preliminary and cursory checks, the PINs and PANs themselves can be phony because the host won't be there to verify legitimacy! That is no legal PINs and PANs need be known nor the algorithm for encrypting PINs. (B) The ATMs message is replaced by a previously recorded legitimate transaction message played back by the phreaker. The cash is dispensed as before. The play back method won't work if the encryption or MA process embed a transaction, clock or random code into the message, making all messages unique. (C) The phreaker/hacker changes the PIN field in the ATMs message to a legitimate PIN of a fat-cat like DONALD TRUMPs account. The phreaker/hacker then withdraws someone else's money. (D) The phreaker/hacker changes the amount field in the ATMs message to a much lower one, and then changes the amount field in the host's message back to the higher amount (debit transactions- the opposite changes are made for credit transactions). So the phreaker can withdraw $200 from his account with only $10 actually debited from it by the host. He can then make many withdrawals before the host cuts him off for exceeding the daily max.

Method 3. TEMPEST IV A thin induction pick-up coil, consisting of many turns of one thickness of #28 or thinner enamel wire sandwiched between two self-adhesive labels, no larger than a debit card, can be inserted at least part way inside the card slot of most ATMs. This coil is then used to "listen in" on the electrical activity inside of the ATM to try to determine which signals control the release of money. Using this same coil as a transmitter

antenna, these signals are then transmitted to the release logic to activate it. It is believed that a thin coil about the size of a dime can be maneuvered quite a ways inside most ATMs for sensing purpose, and that small metal hooks have also been fed into ATMs to obtain direct hookups to logic and power circuits. It is believe that some outlaws have obtained ATM cards. They then machined out the inside of the cards, except the magnetic strip. They then place flat coils inside the machined out area. They then monitor the coils during legitimate transactions. They can also use the coils to transmit desired signals. This is kind of the method used in TERMINATOR 2.

Almost all credit cards now come with either a hologram or an embedded chip ("Smart Card"), and are thus nearly impossible to counterfeit to date. However, since most debit cards are not optically read by ATMs, they are much easier to counterfeit. To counterfeit a card the following is needed: (1) A card embosser, which can be readily obtained from commercial sources (see "Embossing Equipment and Supplies" or similar in the YellowPages) without question asked. A used, serviceable embosser ran $210 + shipping & handling. (2) A magnetic stripe decoder/encoder (skimmer), which can be purchased from the same company as the embossing equipment or just look in the back of Computer Magazines. (3) PIN checkers are not known to be available to the general public. However, if one were stolen, the user could guess at card PINs by trial-and-error effort based upon the knowledge of how PINs are derived. (4) PANs, PINs and ciphers, which can be obtained from a number of ways usually involving theft. About 50% of ATM users write their PINs either on their debit card or somewhere in there wallet or purse. And most user-chosen PINs are easily guessed. The encrypted PINs can be directly lifted or read from the magnetic stripe, and the encryption scheme determined by comparing the encryption with the known PIN # of a dozen or so cards.

BIBLIOGRAPHY

Boyd, John R. "Organic Design for Command and Control." Document M-U 43947-2. Air University Library, May 1987.

Cooper, Pat and Frank Oliveri. "Hacker Exposes United States Vulnerability." Defense News. October 9-15 1995, 1-37.

Fox, Steven G. "Unintended Consequences of Digitization." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1995.

Libecki, Martin "What is Information Warfare?" Institute for National Strategic Studies, World Wide Web page of the National Defense University 1996.

Morton, Oliver. "The Information Advantage." The Economist, June 10, 1995.

Munro, Neil. The Quick and the Dead. New York: St. Martin's Press, 1991.

Rice, M.A. and A.J. Sams. Communications and Information Systems for Battlefield Command and Control. London: Brassey's UK, 1989.

Toffler, Alvin and Heidi Toffler. War and Anti-War. Boston: Little, Brown and Company, 1993.

U.S. Dept. of the Army, Operations, Field Manual 100-5 (Washington: 1993)

U.S. Dept. of the Army, A Statement of the Posture of the United States Army Fiscal Year 1996. Washington 1995.

Woodward, Sandy. One Hundred Days. Annapolis: Naval Institute Press, 1992.

[1] Department of the Army, Operations FM 100-5 (Washington: 1993), 2-10.

[2] Benjamin C. Scharwz, Casualties, Public Opinion & U.S. Military Intervention, (Santa Monica, CA: Rand, 1994), 15, 18,19.

[3] Department of the Army, Operations, FM 100-5 (Washington: 1993), 7-3.

[4] Walter Russell Mead, "The $2 Trillion Mistake," Worth, February 1996, 37.

[5] Insight on the Middle East War (London: Andre Deutsch LTD, 1974), 36.

[6] Yuri Pavlov, Soviet-Cuban Alliance 1959-1991 (New Brunswick: Transaction Publishers, 1994), 227-252.

[7] Department of the Army, Operations, FM 100-5 (Washington: 1993), Glossary 4.

[8] A Statement of the Posture of the United States Army Fiscal Year 1996, Annual Report (Washington D.C.: 1995), 11

[9] Oliver Morton, "The Information Advantage." The Economist, June 10, 1995, 4.

[10] Ibid. 7.

[11] M.A. Rice and A.J. Sams, Communications and Information Systems for Battlefield Command and Control (London: Brassey's UK, 1989), 238

[12] Jason Glashow, "Army seeks to plug digital weak spots," The Army Times, 22 January 1996, 27.

[13] FM 100-5 Glossary 9

[14] John R. Boyd, "Organic Design for Command and Control." Document M-U 43947-2, (Air University Library, May 1987) 26

[15] Steven G. Fox, "Unintended Consequences of Joint Digitization," Unpublished Research Paper, United States Naval War College, Newport, RI: 1995.

[16] Pat Cooper and Frank Oliveri, "Hacker Exposes United States Vulnerability," Defense News, 9-15 October 1995, 1-37.

[17] Pat Cooper, "Internet link to defense data may be too easy," The Army Times, 22 January 1996, 27.

[18] Ibid. 37.

[19] Martin Libecki, "What is Information Warfare?" Institute for National Strategic Studies, (World Wide Web page of the National Defense University 1996).

[20] Dr. Juan Carlos Muiguizur, "The South Atlantic Conflict, an Argentinean point of view," International Defense Review, Vol. 16, No. 2, 1983, 137.

[21] From this "underground" electronic bulletin board I was able to download among other things detailed instructions on defeating the security systems on Automated Teller Machines. The author disclaimed any illegal use of the information but it was rather detailed and technical in its scope. See Appendix B.

[22] Martin Libecki, "What is Information Warfare?" Institute for National Strategic Studies, (World Wide Web page of the National Defense University 1996).

[23] The Information Mission Area Integration Analysis Center (IIAC) currently runs a bulletin board at: http:\\www.army.mil/disc-4-pg/iiac, on which many descriptions of Army STAMIS can be found and also upon which the Army Data Dictionary resides which gives the definitions of all data elements used by the Army. Additionally, the United States Army Information Systems Software Center at Ft. Belvoir publishes a quarterly laydown of all Army STAMIS and how each level talks to and interacts with the other. A potential intruder could learn how a supply STAMIS links up with and talks to a depot system, what communication protocol it uses etc. This information would aid penetration and exploitation.

[24] Virtually every item in the Department of Defense supply system has a National Stock Number (NSN) that identifies it exclusively. These NSNs are linked to noun nomenclatures that are rather cryptic. While stationed in Germany in 1982 as a young lieutenant I once ordered what I thought were Army Good Conduct Medals and the noun nomenclature read medal, set: decoration. The NSN however was for the Medal of Honor. The requisition was canceled of course when the error was realized.

[25] Under current Army Regulation 380-19 Security of Automated Information Systems it is not allowed for a classified network to be connected to an unclassified network. This physical separation of networks makes it very difficult for a hacker to obtain access to a classified system unless he has physical access to a computer terminal connected directly to the network.

[26] The Wall Street Journal, 15 November 1995.